超特異アーベル多様体の定義体と代数曲線の有理点(整数論:保型形式と関連する研究)

AUTHOR(S):

伊吹山, 知義

CITATION:

伊吹山, 知義. 超特異アーベル多様体の定義体と代数曲線の有理点(整数論:保型形式と関連する研究). 数理解析研究所講究録 1990, 727: 53-68

ISSUE DATE:

1990-05

URL:

http://hdl.handle.net/2433/101920

数理解析研究所講究録
第727巻 1990年 53-68

超特異アーベル多様体の定義体と代数曲線の有理点

九州大学教養部　伊吹山　知義　(Tomoyoshi Ibukiyama)

この小文では、very special abelian variety について、Deuring の supersingular elliptic curve の定義体に関する結果を拡張し、その応用として、十分多くの有理点を持つ種数3の代数曲線の存在を示すことを目的とする。前半は桂利行氏との共同研究である。手法は整数論的で、一部、跡公式を用いる。詳しい証明、数値、文献等はプレプリント [6] [5] を参照されたい。

アーベル多様体と「2次形式」(ないし、エルミート形式、4元数的エルミート形式)の整数論は多くの点で密接な関係がある。「2次形式」に関する多くの数論的不変量(格子の類数、自己同型群等)は、それぞれ何らかの幾何学的意味を持っている。たとえばアーベル多様体 A の偏極の同型類とある種の「2次形式」の類数が関係しているのは、A の Néron-Severi 群が古典的な formally real Jordan algebra になっていることからの当然の帰結である。(もちろん具体的に対応関係を書こうと思えば A になん

らかの条件が必要になるし、また結論は自明ではない。この方向の結果としては、たとえば,文献[7]などを参照されたい。)それ以外でも、たとえばmoduli内でのsupersingular abelian surfacesのlocusの規約成分の個数や適当なレベル構造からのガロア群なども「2次形式」の整数論の言葉で記述できる。(文献[8]、[4]参照。)このように幾何学的対象を数論で置き換えるということは、単に見かけの異なるものの間の関係を与えているばかりではなく、幾何学的には計算しにくい量を、手法的には幾何と無縁なコンパクト群上の保型形式の跡公式等の強力な手段で計算できるという点で面白いように思われる。

1 Deuringの結果の復習

標数pの有限素体F_pの代数閉包$\bar{F}_p$上の楕円曲線Eは、p-分点を持たないときsupersingularと呼ばれる。このときは$B = End(E) \otimes_Z Q$とおくとBはちょうどpと∞の分岐するQ上の4元数体であり、$O = End(E)$はその極大整数環になる。一般にBの極大整数環は同型を除いても一意的には決まらないが、その同型類の個数Tは有限であり、Bの類数H以下であることが知られている。この数TのことをBのtype numberという。

定理（Deuring）任意の supersingular elliptic curve は F_{p^2} 上の model をもつ。また、supersingular elliptic curves の $\bar{F}_p$ 上の同型類の個数は H に等しい。このうち F_p 上の model を持つものの個数は $2T-H$ 個である。

ちなみに H と T の具体的な値は Eichler または Deuring によりわかっている。（ここでは省略する。）

2 アーベル多様体に付いての主結果

Shioda, Deligne, Ogus によれば、2 つ以上の supersingular elliptic curves の直積は $\bar{F}_p$ 上、皆同型であることが知られている。以下、n を $n \geq 2$ なる自然数とする。E を supersingular elliptic curve とし $A = E^n$ とする。E としては F_p 上 defined で、しかも F_p 上の Frobenius endomorphism F が $F^2 = -p \cdot id_A$ となるものをとっておくことにする。（このようなものはいつでも存在するし、また前述の結果によればこうとっても本質的な差はない。）以下で扱うのは主偏極アーベル多様体 (A, Θ) であるが、念のために定義を復習しておく。A の *divisors* のなす 1 つの algebraic equivalence class Θ が、effective divisor D で n-fold intersection number $(D^n) = n!$ となる代表をもつとき、Θ を主偏極という。

次に、これと関係する数論的対象を説明する。左B-ベクトル空間B^nは、基底の取り替えを除いて、ただ1つ正定値4元数的エルミート計量をもつ。この計量に付いて、O^nを含む（B^nのmaximal O-latticesの） genusをprincipal genusという。あとの都合のため、もう少し詳しく定義を復習する。Q上の代数群Gを

$$G=\{g\in M_n(B);g^t\bar{g}=n(g)1_n \text{ for some } n(g)\in Q^\times\}$$

で定義する。この代数群のアデール化をG_A、任意のQのplace vについてG_Aのv-成分をG_vで表す。B^n内のleft O-lattice（普通の意味のlatticeでleft O-moduleになるもの）の集合$\mathcal{L}$を次で定義する。

$$\mathcal{L}=\{L:\text{left O-lattice ; for all } v<\infty, L\otimes Z_v=(O_v)^n g_v \text{ for some } g_v\in G_v\}$$

この$\mathcal{L}$をprincipal genusという。$\mathcal{L}$にはGが自然に右から作用しているが、この作用によるG-orbitの個数Hは有限で、これをprincipal genusの類数という。次にG-orbitの完全代表系を$L_1,\ldots,L_H$とする。各i$(1\leq i\leq H)$について$M_n(B)$の部分環R_iを

$$R_i=\{g\in M_n(B);L_ig\subset L_i\}$$

で定義する。いま、ある$g\in G$について$gR_ig^{-1}=R_j$となるとき、R_iとR_jはG-同型と呼ぶことにする。$R_1,\ldots,R_H$のうちで、異なるG-同型類の個数Tを$\mathcal{L}$のtype numberと呼ぶことにする。

主偏極アーベル多様体 (A,Θ) の同型類の個数はHであり、各 L_i $(1 \leq i \leq H)$ と1対1に対応することがわかっている。(cf. [7])

定理1 (with Katsura)
記号を上の通りとすると、アーベル多様体 A の主偏極 Θ は、いつでも F_{p^2} -rational である。さらに、主偏極アーベル多様体 (A,Θ) の内で F_p 上で定義されたmodelをもつようなものの($\bar{F}_p$ 上の)同型類の個数は2T-Hに等しい。

注意:nが小さければHとTは具体的に計算されている。たとえばn=1ならDeuring, Eichlerの古典的な結果である。Hについてはn=2, 3については文献[3], [1], にある。Tについては、n=2ならばTが実はある種の5変数2次形式の類数に等しいことがわかり(cf.[3])、この類数は知られている(Teruaki Asai)ので具体的な値がわかる。結論の式は長くなるのでここでは省略するが、数値例を挙げておく。
下の表で、$n=2$ であり、indecomp./F_p の欄は、F_p 上のmodelをもつΘ がindecomposableな主偏極アーベル多様体の同型類の個数(いいかえると F_p 上のmodelをもつgenus 2のirreducible nonsingular curve Cでその Jacobian variety が E^2 と同型なものの個数)を表す。

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
H	1	1	2	2	5	4	8	10	16	24	36	37	50	55	72	93
$2T-H$	1	1	2	2	5	4	8	8	14	18	18	11	32	19	44	33
$irred./F_p$	0	0	1	1	2	3	5	5	8	12	12	9	22	15	29	26

3 Hecke 作用素

前述の類数 H が群 G の Hecke 作用素の跡を用いて表せること は良く知られているが、実は T もそうである。これを説明して おきたい。(n = 1 の場合は Eichler による。n = 2 の場合は実に すでに [3] に述べておいた。) まず Q の有限素点 v について、G の compact 部分群 U_v を

$$U_v = G_v \cap GL_n(O_v)$$

で定義する。ここで $O_v = O \otimes_Z Z_v$ であり、$GL_n(O_v)$ は $M_n(O_v)$ の (この環の内部で) 可逆な元全部のなす群である。G_A の部分群 U を

$$U = G_\infty \times \prod_{v<\infty} U_v$$

と定義する。通常通り G を diagonal に G_A に埋め込んで、G_A の 部分群とみなす。G_A 上の U に関する weight 0 の保型形式の空間 $\mathcal{M}_0(U)$ は次で定義される。

$$\mathcal{M}_0(U) = \{f : G_A \to C; f(uga) = f(g) \text{ for all } a \in G,\ g \in G_A,\ u \in U\}$$

この空間は有限次元であり、その次元が H である。さて、通常の保型形式論により、一般に G_A 内の U-double coset UgU は $\mathcal{M}_0(U)$ に作用する。(e.g. Hashimoto [2]) すなわち

$$UgU = \coprod_{i=1}^{d} Uh_i \text{ (disjoint)}$$

と片側 coset に分解するとき $f \in \mathcal{M}_0(U)$ について

$$(f|[UgU])(g) = \sum_{i=1}^{d} f(h_i g)$$

とおけば、これは G_A の U-double coset のなす Hecke 環の $\mathcal{M}_0(U)$ への作用になっている。たとえば U-double coset として U 自身をとれば trivial action になる。この作用を普通 $T(1)$ と書くが、あきらかに

$$H = tr(T(1))$$

である。さて次に π を $\mathcal{O}$ の元で $\pi^2 = -p$ となるものとしておく。われわれの E の取り方により、このような元は存在する。G_A の元 $g = (g_v)$ を $g_p = \pi$ かつ $v \neq p$ のとき $g_v = 1$ と定義する。また、$R(\pi) = UgU$ とおく。(簡単のため、$R(\pi)$ で決まる $\mathcal{M}_0(U)$ 上の作用素も $R(\pi)$ とかくことにする。) すると簡単な計算により

$$tr(R(\pi)) = 2T - H$$

がわかる。これらにより、T と H の計算は結局、特殊な Hecke 作用素の跡公式に帰着する。もちろん具体的な計算は一般の n で

は面倒である。なお、念のためにつけ加えると、$R(\pi)$は、いわゆるmultiplicator pのHecke作用素T(p)のうちの一部のdouble cosetだけ取りだした形になっている。つまり、$n \geq 2$では、いつでも$R(\pi) \neq T(p)$である。

4 代数曲線の有理点に付いての主結果

F_{p^2}上の非特異絶対規約代数曲線CのF_{p^2}-有理点の個数に付いては、gをCのgenusとするとき、A.Weilによる評価

$$|\#(C(F_{p^2})) - p^2 - 1| \leq 2gp$$

が良く知られている。しかし、この評価はpまたはgを固定するときbest possibleとは限らない。pを固定したときにgの増大にともない個数がどうなるかに付いてはY.Ihara, Manin等により完全にわかっている。この深い結果に付いてはここでは詳しくは触れないが、結論の一部を借用すれば、pに比較してgが十分大きいときには$\#(C(F_{p^2}))$はWeilの評価の最大値$1+p^2+2gp$を決してattainしない。一方で、J.P.Serreはgを固定すると十分大きいすべてのpについては、最大値をattainするcurveがあるのではないかと問題提起し、また$g \leq 2$については証明も与えている。ここでの新しい結果は次の通りである。

定理 2

p を 3 以上の素数とする。このとき F_p 上定義された genus 3 の irreducible nonsingular curve C で

$$\#(C(F_{p^2})) = 1 + p^2 + 6p$$

となるものが存在する。しかも、p が増大するに従ってこのような curve の（$\bar{F}_p$ 上の同型類の）個数も無限に増大する。

注意 1：p = 2 では正しくない。（Serre） また、この定理は前節の定理からただちにでるわけではない。どこが微妙かは後で説明する。

注意 2：上の curve C が hyperelliptic であるか否かは、一般的にはまったくわからない。（p に適当な条件をつければわかる場合もある。）

5 定理 1 の証明の概要

証明のポイントは定義体に付いての Weil criterion を数論的に書くことにある。そもそも A は F_p 上定義されているのだから、(A, Θ) も有限体上定義されているとして良い。よって、Frobenius endomorphism F についての条件で書ける。まず、Θ が F_{p^2}-rational であるのは $F^2 = -p$ と取ったことから容易に示せる。（ここで

は A の model を取り替える必要もない。) また、(A,Θ) が F_p 上の model を持つための必要十分条件は、D を Θ の F_{p^2}- rational な代表、σ を $Gal(F_{p^2}/F_p)$ の generator とするとき

$$\epsilon(D^\sigma) \approx D \qquad \text{(algebraic equivalence)}$$

となる A の (アーベル多様体としての) automorphism ϵ が存在することである。これを数論的に書き直せば、(A,Θ) と対応する lattice L_i の右 order R_i の p の上にある両側 ideal が G の元で生成されることと同値であることがわかる。(ここでは、一般には A 自身 model を取り替える必要がある。) この性質を持つ R_i の個数と $tr(R(\pi))$ が一致する事がわかり、証明できたことになる。

6 定理2の証明の概要

まず、F.Oort and K.Ueno の結果によれば、任意の3次元主偏極アーベル多様体は、(reducible かもしれない) 'good' curve のヤコービ多様体になっていることが知られている。(もちろん4次元以上では正しくない。これが定理で genus を3に限った主要な理由である。) 従って A の主偏極と principal genus の関係、および n = 1, 2, 3 についての類数公式を用いると、$p \geq 3$ ならば irreducible curve C で $J(C) \cong (A,\Theta)$ ($J(C)$ は C の Jacobian variety) となるものが存在することはわかる。一方、(A,Θ) は F_{p^2} 上定

義されていて、しかも A の Frobenius endomorphism に付いての条件から、Frobenius の固有多項式が $(x^2+p)^3$ となるから、一見 C の F_{p^2}-rational points の個数が $1+p^2+6p$ であることが容易に結論できそうであるが、実際には非常に微妙である。実はこの部分が微妙であるということは 1984 年頃 Serre に教えていただいた。Serre に教わったことは大体次の通りである。

定理（Serre）

一般の主偏極アーベル多様体 $(A,\Theta)/F_{p^e}$ が curve C' のヤコービ多様体と $\bar{F}_p$ 上同型だったと仮定する。このとき、C' の model C で F_{p^e} 上定義されるものがある。さらに、もし C が hyperelliptic なら (A,Θ) と $J(C)$ の間の同型写像も F_{p^e} 上定義されるように取れる。しかし、もし C が non-hyperelliptic ならば、一般には、この同型写像は F_{p^e} 上定義されるように取れるとは限らない。ただし F_{p^e} の 2 次拡大上では定義されているものが取れる。

証明は Torelli の定理による。non-hyperelliptic では Jacobian の自己同型と curve の自己同型が 2 対 1（hyperelliptic では 1 対 1）なので、このような複雑な現象が生じる。一般論としてはこれ以上の結果は望めない。そこで、Serre は hyperelliptic curve でその Jacobian variety が E^3 になるものを見つけると良いという示唆をしてい

る。しかし、私の知る限り、Néron-Severi 群の元を見て（われわれの立場で言えば quaternion hermitian lattice をみて）hyperelliptic か否かを知る有効な手段は見つかっていない。（たとえばテータ因子が singular かどうかというような条件は確かめようがない。）従って、少し別の方策を考えたい。ところで、主偏極アーベル多様体 (A,Θ) で F_p 上の model を持つものを考えると、Jacobian variety との同型が F_{p^2} 上で取れるので、一見うまく行きそうであるが、これも正しくない。model を取り替える同型写像がどこで定義されているかわからないからである。従って、次のようなことがいえれば良いことになる。

定理 3

記号を §2 の通りとする。各素数 $p \geq 3$ について、次の 2 つの条件を満たす主偏極アーベル多様体 (A,Θ) が存在する。

(1) Θ が indecomposable である。

(2) F_p 上の model (A_0,Θ_0) で (A,Θ) と F_{p^2} 上同型なものが存在する。

実際の手続きでは、まず上の条件（2）を満たすものを数えて、それから decomposable のものの個数を引いた値が positive になることを言えば良い。ところで、条件（2）は少なくとも見かけ

上（そして$n \geq 3$ならば、たぶん実際にも）、単にF_p上modelが取れると言うよりも強い条件であって、数論的翻訳が前とは変わってくる。すなわち、（２）と同値な数論的条件は、対応するR_iが$g^2 = -p$かつ$g \in G$なる元を含むということである。このようなR_iの個数を直接、跡公式で求めるのは、少なくともすぐには望めないので、かわりに次のような量を考える。以下では$n = 3$として、前と同様、$L_1, \ldots, L_H$を$\mathcal{L}$の完全代表系とする。各i$(1 \leq i \leq H)$についてGの部分群Γ_iを

$$\Gamma_i = \{g \in G; L_i g = L_i\}$$

で定義する。次に、Hecke作用素の跡公式に良く現れる種類の一種のmassを定義する。すなわち、$M(3)$で次の量を表す。

$$M(3) = \sum_{i=1}^{H} \frac{\#\{g \in G \cap R_i; g^2 = -p\}}{\#(\Gamma_i)}$$

この量は、F_p上のmodelがF_{p^2}上の同型の取り替えで得られるような(A, Θ)の個数を直接与えているわけではないが、右辺の各項は、今の条件を満たす主偏極アーベル多様体でのみ正（つまり、ゼロでない）から、存在定理を示すにはこれで十分役に立つ。ところで、実は$M(3) > 0$となることだけなら非常に簡単にわかるが、ここでは、主偏極がindecomposableかどうかはまったく考慮していないので、これだけではわれわれの目的には遠く及ばない。従って$M(3)$からdecomposableな部分の寄与を引か

ねばならない。$n=1,2$についても同様にmassを定義してそれを$M(1), M(2)$と書き、また

$$M'(3)=\sum_{L_i:indecomposable}\frac{\#(\{g\in G\cap R_i; g^2=-p\})}{\#(\Gamma_i)}$$

とおけば、

$$M'(3)=M(3)-M(1)M(2)+\frac{1}{3}M(1)^3$$

となることが容易にわかる。よって、もし$M'(3)>0$がわかれば目的は達したことになる。masses $M(n)$ (n = 1, 2, 3)は跡公式の計算で具体的に求められる。具体的な$M(3)$等の値を求めるには、もちろん跡公式の長く複雑な計算を必要とし、かなり面倒であるが、ここでは結果のみ述べ詳細は省略する。

定理 4

$M'(3)$の値は次の通り。

(0) $p=3$のとき、

$$\frac{1}{2^3\cdot 3}$$

(1) $p\equiv 1 \bmod 4$のとき、

$$\frac{1}{2^5\cdot 3^2}h(\sqrt{-p})B_{3,\chi}-\frac{1}{2^5\cdot 3}h(\sqrt{-p})^2(4p-1)+\frac{1}{2^3\cdot 3}h(\sqrt{-p})^3$$

(2) $p\equiv 3 \bmod 8,\quad p\neq 3$のとき、

$$\frac{77}{2^4\cdot 3^2}h(\sqrt{-p})B_{3,\chi}-\frac{1}{2^2\cdot 3}h(\sqrt{-p})^2(8p-5)+\frac{8}{3}h(\sqrt{-p})^3$$

(3) $p \equiv 7 \bmod 8$ のとき、

$$\frac{13}{2^4 \cdot 3} h(\sqrt{-p}) B_{3,\chi} - \frac{1}{6} h(\sqrt{-p})^2 (p-1) + \frac{1}{3} h(\sqrt{-p})^3.$$

ここで $h(\sqrt{-p})$ は虚2次体 $Q(\sqrt{-p})$ の類数、χ は $Q(\sqrt{-p})$ に対応する Dirichlet character、また $B_{3,\chi}$ は一般 Bernoulli 数である。一般 Bernoulli 数の簡単な評価をしてみると、この定理4により $p \geq 3$ ならば、$M'(3) > 0$ が示される。また、$\lim_{p \to \infty} M'(3) = \infty$ もわかる。$\#(\Gamma_i)$ は p によらない量でおさえられるので、以上により定理2は示されたことになる。

参考文献

[1] K. Hashimoto. Class numbers of positive definite ternary quaternion hermitian forms. *Proceed. Japan Acad. Ser.A*, 59:490–493, 1983.

[2] K. Hashimoto. On Brandt matrices associated with the positive definite quaternion hermitian forms. *J.Fac.Sci.Univ.Tokyo Sect.IA*, 27:227–245, 1980.

[3] K. Hashimoto and T. Ibukiyama. On class numbers of positive definite binary quaternion harmitian forms. *J.Fac.Sci.Univ.Tokyo Sect.IA Math.*, 27:549–601, 1980.

[4] T. Ibukiyama. On automorphism groups of positive definite binary quaternion hermitian lattices and new mass formula, pages 301–349. *Advanced Studies in pure Math. Vol.15*, Kinokuniya, Tokyo, 1989.

[5] T. Ibukiyama. On rational points of curves of genus three over finite fields. in preparation.

[6] T. Ibukiyama and T. Katsura. On the field of definition of very special polarized abelian varieties and type numbers. 1989. Preprint.

[7] T. Ibukiyama, T. Katsura, and F. Oort. Supersingular curves of genus two and class numbers. *Compositio Math.*, 57:127–152, 1986.

[8] T. Katsura and F. Oort. Families of supersingular abelian surfaces. *Compositio Math.*, 62:107–167, 1987.